UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

JON CARNLEY, JACKIE DENSMORE, PAUL KATYNSKI, JENNIFER KREEGAR, HAROLD MCPHAIL, KATHLEEN PAGLIA, JB SIMMS, and KENNETH TILLMAN, on behalf of themselves and all others similarly situated, Plaintiffs, v. CONDUENT BUSINESS SERVICES, LLC d/b/a DIRECT EXPRESS®, COMERICA, INC., and COMERICA BANK, Defendants.	Case No. 5:19-cv-1075 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs, through undersigned counsel, on behalf of themselves and all persons similarly situated, file this Class Action Complaint, alleging the following based on personal knowledge as to the allegations regarding Plaintiffs and on information and belief as to other allegations:

PARTIES

1. Plaintiff Jon Carnley ("Mr. Carnley") is an Alabama citizen. Mr. Carnley receives federal benefits which are provided to him via his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

2. Plaintiff Jackie Densmore ("Ms. Densmore") is a Massachusetts citizen. Ms. Densmore is the caregiver for her brother-in-law, Derek Densmore, a disabled Marine, who

receives federal benefits which are provided to him through his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank to Ms. Densmore and the program is operated by Conduent Business Services, LLC.

3. Plaintiff Paul Katynski ("Mr. Katynski") is a Nevada citizen. Mr. Katynski receives federal benefits which are provided to him through his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

4. Plaintiff Jennifer Kreegar ("Ms. Kreegar") is an Indiana citizen. Ms. Kreegar receives federal benefits which are provided to her through her Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

5. Plaintiff Harold McPhail ("Mr. McPhail") is a South Carolina citizen. Mr. McPhail receives federal benefits which are provided to him through his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank as part of program operated by Conduent Business Services, LLC.

6. Plaintiff Kathleen Paglia ("Ms. Paglia") is a North Carolina citizen. Ms. Paglia receives federal benefits which are provided to her through her Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

7. Plaintiff JB Simms ("Mr. Simms") is a California citizen. Mr. Simms receives federal benefits which are provided to him through his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

8. Plaintiff Kenneth Tillman ("Mr. Tillman") is a Colorado citizen. Mr. Tillman receives veterans' benefits which are provided to him through his Direct Express® Debit MasterCard Card. The card is issued by Comerica Bank and the program is operated by Conduent Business Services, LLC.

9. Defendant Conduent Business Services, LLC ("Conduent") is a limited liability company organized under the laws of Delaware with its principal place of business located at 2828 N. Haskell Avenue, Building 1, Floor 9, Dallas, Texas 75204. Conduent is publicly traded on the New York Stock Exchange under the ticker symbol "CNDT." Conduent has substantial operations in San Antonio, including an office building housing hundreds of employees at 2822 General Hudnell Drive.

10. Conduent uses the Direct Express® trademark to administer federal benefit payments across the country to benefit recipients of at least nine federal agencies. When Direct Express® customers contact Conduent, they are instructed to write to Conduent at a post office box located in San Antonio, Texas. Conduent's San Antonio office houses substantial operations for the Direct Express® program.

11. Defendant Comerica, Inc. is an entity incorporated under the laws of Delaware with its principal place of business located at Comerica Bank Tower, 1717 Main Street, Dallas, Texas 75201.

12. Comerica is a financial services company that serves millions of customers nationwide. Comerica is publicly traded on the New York Stock Exchange under the ticker symbol "CMA." According to a recent Form 10-K filed with the Securities and Exchange Commission, as of December 31, 2015, Comerica was among the 25 largest commercial bank holding companies in the United States.

13. Comerica Bank offers a broad array of retail, small business, and commercial banking products.

14. Defendant Comerica Bank is chartered by the State of Texas and has numerous branches throughout the State of Texas, including several in San Antonio. Defendants Comerica Bank and Comerica, Inc. are sometimes collectively referred to hereinafter as "Comerica."

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331. Jurisdiction is also proper pursuant to the Class Action Fairness Act (28 U.S.C. § 1332(d)) because the claims of the proposed class when aggregated together exceed $5,000,000 and some putative class members are residents of different states than Defendants.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Conduent and Comerica have their principle places of business in the State of Texas and utilize San Antonio as the location of their customer service center. Indeed, Conduent and Comerica administer various state assistance programs in Texas. Thus, Defendants have substantial business operations within the Western District and could reasonably be expected to be hauled into Court in this District.

PROCEDURAL BACKGROUND

17. Plaintiffs originally filed against Defendants on or about February 12, 2019 in the United States District Court for the Northern District of Georgia, in a case styled *Almon v. Conduent Business Services, LLC, et al.*, Case No. 1:19-cv-00746-LMM.

18. On August 9, 2019, the District Court in *Almon* issued an order allowing only the Georgia customers to proceed in Georgia. The claims of Plaintiffs in this action – all of whom live outside of Georgia – were dismissed for lack of jurisdiction.

19. Plaintiffs hereby promptly renew their claims against Defendants.

COMMON FACTUAL ALLEGATIONS

20. Comerica originally won the government contract to oversee the Direct Express® benefits program in 2008.

21. The contract was renewed in 2014 despite some criticism by the Treasury's Office of Inspector General ("Inspector General") over how the program was being run.

22. The Inspector General's concerns over how Comerica was running the program resulted from audits performed on the program.

23. In June 2018, the Inspector General issued an "engagement memo" to Treasury related to the Direct Express® program.

24. The memo informed the Bureau of the Fiscal Service of a follow-up audit to determine if program administrators had responded to 14 recommendations included in 2014 and 2017 Inspector General audits.

25. Among the recommendations included in the audits was that the Direct Express® program make an assessment of the costs and burdens of the program on the cardholders; establish a quality assurance surveillance plan to monitor and document Comerica's performance, including service-level requirements; track Comerica's revenues and expenses; and periodically assess whether the bank's compensation is "reasonable and fair."

26. In August 2018, in an interview with Kate Berry from the American Banker, Comerica senior vice president and director of government electronic solutions Nora Arpin admitted that the Direct Express® program's security programs had been breached.

27. Ms. Arpin acknowledged that "[c]riminals have found a way around the controls that we put in place to safeguard cardholders."

28. Ms. Arpin further stated that Defendants took action "to shut down the Cardless Benefit Access Service[1] and have begun an investigation."

29. At the same time the American Banker was running its story in August 2018 regarding the Direct Express® program, Senator Elizabeth Warren was also conducting an investigation into Comerica and Conduent.

30. Senator Warren's office, along with Representative William Keating's office, were contacted by Plaintiff Jackie Densmore, after her efforts to communicate with Direct Express® directly regarding the fraudulent transactions on her brother-in-law's account fell on deaf ears.

31. Senator Warren's initial findings were detailed in a letter to the Department of Treasury that stated:

> Since 2008, Comerica Bank has contracted with the Department of Treasury to administer the Direct Express® program, which provides prepaid debit cards and electronic payments of federal benefits such as social security, disability, and veteran benefits. 4.5 million Americans utilize Comerica's Direct Express® program, and Direct Express® dispersed around $3 billion in Social Security and SST payments to 4.3 million Americans in September 2018. As of October 2018, Direct Express® distributed nearly $90 million in benefits to nearly 84,000 veterans or their families.
>
> I opened this investigation as a result of numerous complaints from my constituents and detailed reports in *American Banker* that revealed allegations for fraud in a feature of the Direct Express® program known as the Cardless Benefit Access Service. As part of the investigation, I wrote to Comerica, the Social Security Administration (SSA), and the Department of Veterans Affairs (VA), receiving written responses from all three. In addition, my staff received briefings from Comerica and the Department of the Treasury's Office of Inspector General (OIG).
>
> The Cardless Benefit Access feature, which Comerica originally called "Emergency Cash," was designed to allow Direct Express® cardholders who lost or did not have their physical debit card to request and transfer money to a MoneyGram location, often out of state. The feature was introduced to all Direct Express® cardholders in August 2017 and proved to be valuable in the aftermath of Hurricanes Harvey and Maria. Direct Express® cardholders in affected areas were

[1] The Cardless Benefit Access Service is a feature of the Direct Express® program that allows cardholders to access their benefits even when their card is not in their possession.

able to obtain emergency funds from MoneyGram locations operating on generators as a result of the hurricanes, even if ATMs in the area were out of service or if cardholders had left their cards behind to escape the hurricanes and flooding.

Because of concerns about targeted fraud, the feature was suspended in August 2018, and in October 2018, Comerica stated that the Cardless Benefit Access feature "has been suspended temporarily . . . but has not been discontinued as it has been a lifeline for many [Direct Express] cardholders."

My investigation revealed the following new information about the explanation for, scope of, and response to the fraud:

- **Hundreds of individuals were affected by fraud in the Direct Express® program.**

. . .

- **SSA and VA officials and the public were not adequately informed of fraud affecting their program beneficiaries.**

. . .

- **There are multiple ongoing investigations of the Direct Express® fraud schemes and of other aspects of the Direct Express® program.**

. . .

32. Ultimately, Senator Warren concluded:

If functioning properly, there is unquestionable value in the Direct Express® program – it gives financial freedom and agency to millions of elderly and disabled Americans. But these Direct Express® customers are particularly vulnerable. The Direct Express® program was designed for individuals who don't have bank accounts, and for many of these Americans their federal benefits are their sole source of income that keep a roof over their head, pay for life-saving medications, and put food on the table. The importance of the security and proper implementation of your agency's government-contracted program cannot be understated.

I urge you to take the facts and information gathered through my investigation into consideration during the Direct Express® financial agency contract bidding process and to modify the new contract language to ensure improvements in the financial agent's ability to prevent and respond to fraud schemes or security vulnerabilities.

33. As demonstrated herein, the fraud reported to Senator Warren with respect to the Cardless Benefit Access Service program is just the tip of the iceberg.

34. For example, many Direct Express® customers who did not participate in the Cardless Benefit Access Service program – like many of the Plaintiffs – also experienced fraudulent transactions that Defendants failed to address.

35. Defendants tout the Direct Express® card as a prepaid debit card offered to federal benefit recipients who receive their benefits electronically.

36. According to Defendants, "[t]he debit card offers the convenience and ***security*** of using electronic transactions to spend and access your money rather than using cash for purchases." (emphasis added).

37. Defendants encourage federal benefits recipients to enroll in the Direct Express® card program because recipients "will receive [their] payment every month without having to worry about cashing your check or ***having it lost or stolen***. Instead of receiving a check, your money will be automatically deposited to your Direct Express® card account on payment day." (emphasis added).

38. Defendants assure federal benefit recipients like Plaintiffs that their social security, supplemental security income, veterans benefits, and other federal benefits are safe, claiming:

> with the Direct Express® card, your money is FDIC-insured up to the maximum legal limit. In addition, the consumer protections required by Regulation E (12 CFR 1005) and MasterCard® Zero Liability (exceptions may apply), ***protects you against unauthorized use of your card***. When promptly reported, this will apply to your debit card account.

(emphasis added).

39. Defendants also publicize to federal benefit recipients that one of the benefits of having a Direct Express® Card is that "***It's Safe: No need to carry large amounts of cash and no risk of lost or stolen checks.***" (emphasis added).

40. Thus, despite knowing of all the problems with fraud highlighted by Senator Warren and the American Banker, Defendants misrepresent to their customers that the Direct Express® program is completely safe.

41. Plaintiffs and the members of the proposed classes reasonably rely on Defendants' statements regarding the safety of their Direct Express® cards.

42. In reality, Direct Express® cards are unsafe, having negligible security protections or fraud alert capabilities, and Defendants' systems are rife with fraudulent transactions.

43. Indeed, in a recent Interim Audit Update released by the Department of the Treasury on July 29, 2019 (OIG-19-041), the Audit Director indicated that the call center created by Defendants to respond to fraud claims made by customers "has received poor ratings in some categories such as customer service representative response times and regulatory compliance related to chargeback and dispute processing."

44. The Interim Audit Update also stated that Defendants needed to "[i]mprov[e] the customer experience and compliance with Regulation E" in order to increase the public trust in Direct Express® program.

FACTUAL ALLEGATIONS RELATING TO BREACH OF CONTRACT AND REGULATION E CLAIMS

45. When benefit recipients like Plaintiffs receive their debit card, Conduent and Comerica allegedly provide them with a Direct Express® Debit MasterCard Card Terms of Use that ostensibly outline the terms and conditions that govern use of the debit card. A representative copy of the Terms of Use issued by Conduent and/or Comerica is attached hereto as Exhibit A.

46. It is possible that discovery may show that additional versions of the Terms of Use exist and were perhaps effective during other portions of the likely class period. Thus, Exhibit A hereto is not offered as the definitive contract for all relevant class members or time periods.

47. The standardized Terms of Use were presented to Plaintiffs and other benefit recipients on a "take it or leave it" basis, and card holders are often not informed that they have any other option to receive their funds. The form contract was drafted and imposed by Conduent and/or Comerica, which is the party of vastly superior bargaining strength, indeed no bargaining is allowed. Customers are not allowed to negotiate or make a single change to the document. The Terms of Use constitute an agreement of adhesion.

48. The Terms of Use contain detailed procedures of what a cardholder is supposed to do if they believe their debit card has been lost or stolen or that someone has unlawfully transferred money from their debit card. See Exhibit A, ¶ VII.

49. For example, the Terms of Use advise card users as follows:

> You agree not to give or otherwise make available your Card or PIN available to others. If you do, you will be responsible for any Transactions they conduct, even if they exceed your authorization. For security reasons you agree not to write your PIN on your Card or keep it in the same place as your Card.
>
> If you believe your Card or PIN has been lost or stolen or that someone has transferred or may transfer money from your available funds without your permission, report it by calling the Customer Service number below as soon as possible. You can also write to us at Direct Express®, Payment Processing Services, P.O. Box 245998, San Antonio, Texas 78224-5998 or visit our website at www.USDirectExpress.com.

See Exhibit A, ¶ VII.

50. The Terms of Use also advise card users that in the case of errors or questions about their transactions the following shall apply:

> Call the Customer Service number below or write to use at the address described below as soon as you can if you think an error has occurred in your Card Account.

> We must hear from you no later than 90 days after you learn of the error. You will need to tell us:
> a. Your name and Card number.
> b. Why you believe there is an error, and the dollar amount involved.
> c. The approximately date when the error took place.
>
> Please provide us with your street address, email address, and telephone, as well, so that we can communicate with you.
>
> If the error cannot be resolved over the phone, you must provide us written notice of the error with 10 business days at Direct Express® Payment Processing Services, P.O. Box 245998, San Antonio, Texas 78224-5998.
>
> We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days to investigate your complaint or question. If we decide to do this, we will credit your Card within 10 business days (20 business days for new card accounts after the first deposit is made to the Card) for the amount you think is in error, so that you will have use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your Card. For errors involving new Cards, point-of-sale, or foreign-initiated transactions, we may take up to 90 days to investigate your complaint or question.
>
> We will tell you the results within three Business Days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation.
>
> If you need more information about our error-resolution procedures, call us at the Customer Service number below.

See Exhibit A, ¶ IX.

51. The Terms of Use also state the following regarding Defendants' liability with respect to fraudulent or unauthorized transactions on their accounts:

> Tell us AT ONCE if you believe your Card or PIN has been lost or stolen. Telephoning us at the Customer Service number is the best way of keeping your possible losses down. You could lose all the money associated with your Card. If you tell us within two business days, you can lose no more than $50 if someone used your Card or PIN without your permission. If you do NOT tell us within two (2) Business Days after you learn of the loss or theft of your Card or PIN, and we can prove that we could have stopped someone from using your Card or PIN without your permission if you had told us, you could lose as much as $500.

> …
>
> Also, if the written transaction history or other Card transaction information provided to you shows transfers that you did not make, tell us at once. If you do not tell us within 90 days after the transmittal of such information, you may not get back any money you lost after the 90 days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or a hospital stay) kept you from notifying us, we will extend the time periods.

See Exhibit A, ¶ VIII.

52. Despite the clear language in the Terms of Use with respect to (1) the procedures that cardholders must follow regarding lost or stolen cards and unauthorized activity, and (2) the limitations on a cardholders' liability for fraudulent charges and unauthorized uses, Defendants routinely ignore these contractual obligations in direct violation of the Terms of Use.

53. Instead of following the procedures outlined in the Terms of Use, Defendants engage in a pattern of conduct that includes sham investigations and improper denial of meritorious claims regarding fraudulent charges and unauthorized uses.

54. Further, Defendants ignore the limitations of liability language contained in the Terms of Use and leave the users of the Direct Express® Debit MasterCard Card holding the bag on hundreds, thousands, and even tens of thousands of dollars of fraudulent charges by unauthorized persons.

55. Plaintiffs' experiences with Defendants illustrate this reality.

56. Plaintiff Mr. Carnley receives federal benefits through his Direct Express® Debit MasterCard Card.

57. On January 3, 2019, Mr. Carnley purchased a money order at the Andalusia, Alabama Walmart for $464.88.

58. Unbeknownst to Mr. Carnley, an ATM cash withdrawal of $182.50 was made from his card in an Arizona Walmart within seconds of him purchasing the money order in Alabama.

59. Five days later, on January 8, 2019, a duplicate money order was purchased using Mr. Carnley's card information at the Walmart in Andalusia, Alabama for $464.88.

60. Mr. Carnley could not have made this second money order request because starting on January 6, 2019 he was in Pensacola, Florida preparing to go to MD Anderson Hospital in Houston to begin cancer treatment.

61. On January 15, Mr. Carnley called the number on the back of his Direct Express® card regarding the $464.88 fraudulent charge.

62. Defendants refused to provide Mr. Carnley a provisional credit or do anything to stop the fraudulent transactions from draining his benefits account.

63. On January 16, Mr. Carnley again contacted Direct Express®, this time about the fraudulent ATM withdrawal in Arizona.

64. During his conversation with a Direct Express® customer service agent named David, Mr. Carnley was informed that the New Jersey office had been compromised and there had been a data breach.

65. The aforementioned charges are not the first time Mr. Carnley's Direct Express® card has been used fraudulently.

66. Mr. Carnley also was the victim of fraudulent charges on his Direct Express® card in August and November 2018. These earlier fraudulent charges totaled almost $550.

67. Defendants refused to provide Mr. Carnley with the results of their purported investigation in a timely fashion, failed to provide Mr. Carnley a provisional credit, and failed to do anything to stop fraudulent transactions from draining his benefits account.

68. Moreover, Defendants failed to limit Mr. Carnley's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

69. Plaintiff Ms. Densmore is the caregiver for her brother-in-law, Derek, a disabled Marine who receives veterans benefits through a Direct Express® Debit MasterCard Card.

70. Even though Ms. Densmore did not use the "Cardless Benefit Access Service," an unknown individual or individuals were able to utilize this service to withdraw $814 from Derek Densmore's Direct Express® account via a MoneyGram to a Walmart Superstore in Hollywood, Florida even though the Densmores reside in Massachusetts.

71. On August 3, 2018, Ms. Densmore called the number on the back of the Direct Express® card to see if Derek's monthly benefits had been deposited into his account.

72. Ms. Densmore received a recording informing her that a new Direct Express® card had been mailed out.

73. After waiting a couple of days to see if the new card arrived, Ms. Densmore tried to contact Direct Express® about the new card.

74. After trying unsuccessfully to get someone on the phone that could assist her, on August 10, 2018, Ms. Densmore was finally able to reach a supervisor.

75. The supervisor stated that someone had called Direct Express® on August 2, 2018, claiming to be Ms. Densmore (even providing her name, address, and social security) stating that they had damaged the card and wanted Direct Express® to send a MoneyGram so they could access the funds.

76. Ms. Densmore advised the supervisor that neither she nor her disabled brother-in-law had made such a request.

77. The supervisor stated that a fraud claim was being opened and that Ms. Densmore needed to fill out paperwork and return it back to Direct Express® so that the fraud department could investigate.

78. After Direct Express® failed to send Ms. Densmore the paperwork needed to dispute the fraudulent charges, Ms. Densmore put together a hand-written narrative outlining the fraudulent transaction that her brother-in-law's account had experienced and submitted it to Direct Express® via facsimile.

79. Over the next few weeks, Ms. Densmore contacted Direct Express® on numerous occasions about the fraudulent withdrawal from her brother-in-law's account, but Direct Express® refused to reimburse the funds to the account.

80. As they did with the rest of Plaintiffs, Defendants refused to provide Ms. Densmore with the results of their purported investigation in a timely fashion, failed to provide Ms. Densmore a provisional credit, and failed to do anything to stop fraudulent transactions from draining her brother-in-law's benefits account.

81. Moreover, Defendants failed to limit Ms. Densmore's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

82. Plaintiff Mr. Katynski is a disabled maintenance supervisor who receives disability benefits through his Direct Express® Debit MasterCard Card.

83. In February 2018, Mr. Katynski contacted Direct Express® to check the balance on his account.

84. Instead of being able to check his balance, Mr. Katynski heard a recorded message that informed him that the PIN that he entered did not match Direct Express® records.

85. After receiving that message, Mr. Katynski reset his PIN.

86. Subsequently, Mr. Katynski learned that $1,971 in disability benefits had been drained from his account.

87. Mr. Katynski immediately called Direct Express® which informed him that he had reported the card as lost.

88. Mr. Katynski disputed that claim and informed Direct Express® that he had his card in his possession.

89. Direct Express® shipped out a new prepaid card and gave Mr. Katynski the tracking number for his new card.

90. The next day, Mr. Katynski called to get a delivery update on his card only to discover that the card had been re-routed to an address in Miramar, Florida rather than delivered to him in Nevada.

91. A subsequent call to Direct Express® allowed Mr. Katynski to cancel this second card and avert further fraud.

92. To avoid missing his rent payment, Mr. Katynski requested that Direct Express® send him money via MoneyGram.

93. Direct Express® agreed, but charged him $59 in fees for purportedly receiving and activating two new cards, as well as receiving two MoneyGrams that he needed to pay his rent.

94. Despite Mr. Katynski immediately contacting Direct Express® regarding the fraudulent transactions, Defendants refused to provide him a provisional credit, failed to timely provide Mr. Katynski with the results of their purported investigation, or do anything to stop the fraudulent transactions from draining his benefits account.

95. Moreover, Defendants failed to limit Mr. Katynski's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

96. Plaintiff Ms. Kreegar is a military veteran that receives monthly veterans benefits for a service-related injury through a Direct Express® Debit MasterCard Card.

97. On December 30, 2018, Ms. Kreegar checked her balance, hoping her benefits would be deposited early because this was a holiday weekend.

98. She saw a $13.50 charge on her account, for an expedited item fee that she did not recognize.

99. Ms. Kreegar checked her account again on the following day. She noticed a withdrawal from an ATM located at 154 South Main Street ($1,003.00) and Village Square Shopping Center ($123.00).

100. Neither of these withdrawals were made by Ms. Kreegar.

101. Ms. Kreegar called Direct Express® to dispute these transactions and to request her card be cancelled.

102. That same day, December 31, 2018, Ms. Kreegar received a post card. It was postmarked from Addison, Texas on December 27, 2018, had no return address or other sender identification, but had printed "address update on your debit card on 12/06/2018 at 06:31PM," indicating the postcard was mailed by Conduent/Direct Express® 21 days after the fraudulent address change.

103. Of course, Ms. Kreegar had not changed her address, but rather criminals had successfully changed her address and had a new card sent out, resulting in the fraudulent charges on her account and in the $13.50 charge for an expedited item – namely a replacement card for the criminals to utilize.

104. As a result of Defendants' negligence, Ms. Kreegar's veterans benefits account was compromised and she lost substantial funds.

105. Plaintiff Mr. McPhail is a retired, disabled veteran who receives his federal benefits through a Direct Express® Debit MasterCard Card.

106. In May 2018, after receiving inpatient treatment in a Skilled Nursing Facility on April 17, 2018, Mr. McPhail noticed that several unauthorized transactions had occurred on his Direct Express® account while he was receiving inpatient medical care. These transactions occurred at 01:01:30 and 01:16:06 on April 17, 2018.

107. While reviewing his April 2018 account statement, Mr. McPhail discovered the following transfers had been made from his account to a "Green Dot Card:"

- April 04, 2018 $7,000
- April 17, 2018 $6,000
- April 17, 2018 $4,000

108. On May 11, 2018, Mr. McPhail initiated an investigation for the $17,000 in fraudulent transactions by calling Direct Express®.

109. In response to his phone call, Direct Express® sent Mr. McPhail a letter from the Fraud Services Department along with a "Questionnaire of Fraud" to complete.

110. Mr. McPhail immediately completed and returned the Questionnaire back to Direct Express®.

111. In response, Mr. McPhail received a letter dated June 25, 2018, which stated:

> During the investigation we found a conflict in the information provided by you and the information resulting from our research. Based on this information, we cannot confirm that fraud occurred. You may request a copy of the documents in which we relied in making our determination by contacting us at 1-888-741-1115.

112. This letter also advised Mr. McPhail to contact his local police department, which Mr. McPhail did and ultimately filed a police report.

113. Mr. McPhail also contacted the number provided and requested the documents that supported the denial of his claim.

114. During that conversation, an agent of Direct Express® informed Mr. McPhail that his fraud claim was denied because "the same type of transaction occurred in February and March 2018, which Mr. McPhail had not noticed and failed to dispute."

115. On July 14, 2018, Mr. McPhail filed another fraud claim with Direct Express®, this time regarding a $6,000 transaction dated February 13, 2018 and a $7,000 transaction from March 6, 2018.

116. A letter and "Questionnaire of Fraud" were again sent out from Direct Express®.

117. Mr. McPhail again completed the claim form and returned the package within the requisite 10 business days. Mr. McPhail's submission included a copy of the police report that he had filed with the Darlington County Sheriff's Department.

118. Subsequently, Mr. McPhail received a letter dated Aug 14, 2018 that once again denied his claim.

119. This denial letter was simply the same form letter that Mr. McPhail had been sent previously regarding his earlier claim and did not even acknowledge the police report that had been submitted.

120. In response to the second denial letter, Mr. McPhail again contacted Direct Express® and requested a copy of the documentation relied upon to deny his claim.

121. Defendants have failed to provide Mr. McPhail with a copy of the documents on which they relied in making their determination to deny either of his claims.

122. Further, despite Mr. McPhail promptly contacting Direct Express® regarding the fraudulent transactions, Defendants refused to provide him a provisional credit, and failed to timely provide Mr. McPhail with the results of their purported investigation.

123. Moreover, Defendants failed to limit Mr. McPhail's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

124. As of the filing of this complaint, Mr. McPhail has lost $30,000 to fraudulent transactions that Defendants have refused to refund.

125. Plaintiff Ms. Paglia receives monthly social security benefits through a Direct Express® Debit MasterCard Card.

126. At midnight on March 13, 2019, Ms. Paglia received her monthly deposit from the Social Security Administration onto her Direct Express® card.

127. A mere 26 minutes after she received her monthly benefits, Ms. Paglia's account was hit with an $803.00 withdrawal from an ATM located at 6015 Washington Street in Hollywood, Florida.

128. Less than one-minute later, a second ATM withdrawal was made from Ms. Paglia's account, this time for $123.00 at the same location.

129. Several hours later, Ms. Paglia's account was hit with a $6.42 charge from a Burger King in Miami, Florida.

130. None of these ATM withdrawals or purchases were made by Ms. Paglia.

131. Ms. Paglia discovered that these fraudulent charges had been made on March 16, 2019, when she attempted to make a purchase, but the purchase was declined due to an incorrect PIN number.

132. That same day, after resetting her PIN, Ms. Paglia went to an ATM to check her balance. When she checked her balance, she learned that her account had been drained of nearly all funds due to the aforementioned ATM withdrawals and Burger King purchase on March 13.

133. On March 16, 2019, Ms. Paglia contacted Direct Express® to dispute the fraudulent charges.

134. Defendants responded by sending Ms. Paglia a Questionnaire of Fraud form to fill out to dispute the charges. After receiving the Questionnaire of Fraud on March 26, 2019, Ms. Paglia filled out and returned the form to Defendants via facsimile on March 27, 2019.

135. Much to Ms. Paglia's surprise, she received a letter dated March 29, 2019 that claimed that a thorough investigation had been conducted and that Direct Express® could not confirm fraud had occurred, and therefore her claim was being denied.

136. Ms. Paglia also received a second letter, dated April 1, 2019, which also indicated that her fraud claim was being denied.

137. Upon receipt of the letter, Ms. Paglia contacted Defendants and requested a copy of the documents on which they relied in making this determination.

138. Defendants have failed to provide Ms. Paglia with a copy of the documents on which they relied in making their determination to deny her fraud claim.

139. Further, despite Ms. Paglia promptly contacting Direct Express® regarding the fraudulent transactions, Defendants refused to provide her a provisional credit, and failed to timely provide Ms. Paglia with the results of their purported investigation.

140. Moreover, Defendants failed to limit Ms. Paglia's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

141. As a result of Defendants' conduct, Ms. Paglia's account was compromised and she lost substantial funds.

142. Plaintiff Mr. Simms's veterans' benefits are provided to him through his Direct Express® Debit MasterCard Card.

143. In January 2017, Mr. Simms discovered fraudulent transactions were made on his account, namely, the purchase of Caribbean vacation packages.

144. Mr. Simms disputed these transactions with Direct Express® and was informed that he would be sent a "fraud packet" so that he could formally dispute these charges.

145. While Direct Express® did not deliver the Questionnaire of Fraud to Mr. Simms in a timely manner; Mr. Simms timely mailed a written narrative outlining the fraudulent transactions to Direct Express®.

146. Ultimately, Defendants denied Mr. Simms' fraud claim.

147. Despite Mr. Simms' request, Defendants failed to provide Mr. Simms with a copy of the documents upon which they relied in making their determination that the transactions were not fraudulent.

148. Defendants also failed to limit Mr. Simms's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

149. Mr. Simms was victimized by fraudulent transactions a second time in December 2017.

150. On this occasion, Mr. Simms discovered an unauthorized pending charge on his account and immediately reported the fraud to Direct Express® via facsimile.

151. Defendants denied Mr. Simms fraud claim a second time and failed to provide Mr. Simms with a copy of the documents on which they relied in making their determination to once again deny his claim.

152. Further, despite Mr. Simms promptly contacting Direct Express® regarding the fraudulent transactions, Defendants refused to provide him a provisional credit, and failed to timely provide Mr. Simms with the results of their purported investigation.

153. Moreover, Defendants failed to limit Mr. Simms's losses to either $50 or $500 as required under the Terms of Use applicable to Direct Express® Cards.

154. Plaintiff Mr. Tillman is a military veteran that receives monthly veterans' benefits through a Direct Express® Debit MasterCard Card.

155. On August 1, 2018, Mr. Tillman attempted to withdraw $100 cash from his Direct Express® account at the King Soopers Supermarket on Martin Luther King Boulevard in Denver, Colorado.

156. This transaction was declined twice based on insufficient funds.

157. Mr. Tillman immediately attempted to contact Direct Express® to get to the bottom of why his request to withdraw $100 was denied for insufficient funds.

158. After unsuccessfully trying to reach someone at Direct Express® on the phone for several hours, Mr. Tillman, with the assistance of his therapist, was finally able to get a customer service representative on the telephone.

159. The customer service representative advised Mr. Tillman that his account had insufficient funds based on the following three transactions: a charge for $427.22 at Walgreens Store #3383 at 141 Kearny Street in San Francisco, California; a charge for $283.71 at Walgreens Store #4680 at 730 Market Street in San Francisco; and a $10.00 charge at the High Street Laundromat at 3401 High Street in Oakland, California.

160. Since Mr. Tillman was in Colorado and had not made, or otherwise authorized, these transactions in California, he reported these transactions as fraudulent.

161. The customer service representative acknowledged to Mr. Tillman that these transactions were fraudulent and agreed to cancel his Direct Express® card.

162. Mr. Tillman was then advised to call back on Monday to get an update on these fraudulent transactions.

163. When Mr. Tillman called back on Monday, he was advised that it could take up to 90 days to receive a refund for the fraudulent transactions, if Direct Express® determined they were indeed fraud.

164. Ultimately, Defendants failed to timely provide Mr. Tillman with the results of their purported investigation into his fraud claim and failed to provide him with a provision credit while investigating his claim.

165. Plaintiffs' experiences and those of other victims demonstrate that Defendants systematically refuse to honor their agreements, including by failing to provide refunds to Direct Express® users who experience fraud on their accounts.

166. Plaintiffs' experiences and those of other victims also demonstrate that Defendants conduct pre-textual, sham investigations so that they can improperly deny of meritorious claims regarding fraudulent charges.

167. Defendants' refusal to provide refunds to Plaintiffs and other victims saves them millions of dollars each year but wrongfully deprives their customers of funds that rightfully belong to them.

FACTUAL ALLEGATIONS RELATING TO DATA BREACH CLAIMS

168. As noted above, in an August 2018 interview with Kate Berry from the American Banker, Comerica senior vice president and director of government electronic solutions Nora Arpin admitted that the Direct Express® program's security programs had been breached. Ms. Arpin was quoted as saying "[c]riminals have found a way around the controls that we put in place to safeguard cardholders."

169. Additionally, during a conversation with a Direct Express® customer service agent named David, Plaintiff Jon Carnley was told by David that Conduent's New Jersey office had been compromised and there had been a data breach.

170. Because Conduent and Comerica are administering a federal benefits program for the U.S. Department of the Treasury, Defendants have been entrusted with sensitive personal information for cardholders such as their social security numbers, address, date of birth, Direct Express® account number, and the pin number a cardholder has either chosen or been given to access their account.

171. As a result of the data breaches admitted by agents of Defendants, criminals gained access to the aforementioned sensitive personal information that cardholders had entrusted Conduent and Comerica to safeguard.

172. By gaining access to the aforementioned sensitive personal information, criminals obtained all the information necessary to conduct fraudulent transactions on cardholders' accounts such as unauthorized money transfers, or requesting duplicate or replacement cards that could be used to make unauthorized purchases.

173. As a result of the data breaches acknowledged by Defendants, Plaintiffs and those similarly situated were victims of fraudulent transactions on their Direct Express® accounts.

174. Defendants' failure to adequately safeguard the sensitive personal information entrusted to them by Plaintiffs and other victims resulted in the wrongful deprivation of funds that rightfully belong to Plaintiffs and those similarly situated.

CLASS ALLEGATIONS

175. Plaintiffs bring this action on behalf of themselves and all others similarly situated pursuant to Federal Rule 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23.

176. Plaintiffs seek to represent three Classes of similarly situated people. The proposed Classes are defined as:

> All Conduent and Comerica DirectExpress® Debit MasterCard Card customers in the United States who, within the applicable statute of limitations period preceding the filing of this action and through the date of class certification, incurred fraudulent charges on their accounts and were denied a refund of such charges in violation of Defendants' Terms of Use (the "Breach of Contract Class").
>
> All Conduent and Comerica DirectExpress® Debit MasterCard Card customers in the United States who, within the applicable statute of limitations period preceding the filing of this action through the date of class certification, were not refunded for fraudulent transactions on their account in accordance with 15 U.S.C. § 1693f (the "Regulation E Class").
>
> All Conduent and Comerica DirectExpress® Debit MasterCard Card customers in the United States who, within the applicable statute of limitations period preceding the filing of this action through the date of class certification, had their personal information compromised as a result of a data breach experienced by Defendants (the "Data Breach Class").

177. Plaintiffs also seek to certify the subclasses for violations of the consumer protection statutes of the states of Alabama, California, Colorado, Massachusetts, Nevada, North Carolina, and South Carolina.

178. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

179. Excluded from the Classes are Conduent, Comerica, their parents, subsidiaries, affiliates, officers, and directors, any entity in which Conduent and/or Comerica have a controlling

interest, all customers who make a timely election to be excluded, governmental entities, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

180. The members of the Classes are so numerous that joinder is impractical. The Classes consists of thousands of members whose identity is within the knowledge of Conduent and Comerica and can be ascertained only by reviewing the records of Conduent and Comerica.

181. The claims of the representative Plaintiffs are typical of the claims of the Classes in that Plaintiffs, like all Class members, lost funds based on the improper practices described herein. The representative Plaintiffs, like all Class members, have been damaged by the misconduct of Conduent and Comerica. Furthermore, the factual basis of Defendants' misconduct is common to all Class members, and represents a common thread of conduct resulting in injury to all members of the Classes.

182. There are numerous questions of law and fact common to the Classes and those common questions predominate over any questions affecting only individual Class members.

183. Among the questions of law and fact common to the Classes are whether Defendants:

a. Violate the express language of the Terms of Use;

b. Breach the covenant of good faith and fair dealing through their practices;

c. Require their customers to enter into standardized account agreements which include unconscionable provisions;

d. Violate Regulation E (15 U.S.C. § 1693, *et seq.*) through their practices;

e. Conduct sham investigations into fraud claims as a pretext so that they can deny said claims; and

f. Failed to prevent various data breaches and adequately alert their customers of these breaches.

184. Other questions of law and fact common to the Classes include:

a. The proper method or methods by which to measure damages, and

b. The declaratory relief to which the Classes are entitled.

185. Plaintiffs' claims are typical of the claims of other Class members, in that they arise out of the same wrongful policies and practices and the same or substantially similar provisions of Defendants' form agreements and other related documents. Plaintiffs have suffered the harms alleged and have no interests antagonistic to the interests of any other Class members.

186. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in the prosecution of class actions and, in particular, class actions on behalf of consumers against financial institutions. Accordingly, Plaintiffs are adequate representatives and will fairly and adequately protect the interests of the Classes.

187. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Since the amount of each individual Class member's claim is small relative to the complexity of the litigation, and due to the financial resources of Conduent and Comerica, no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the Class members will continue to suffer losses and Defendants' misconduct will proceed without remedy.

188. Even if Class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a

class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CLAIM FOR RELIEF

Breach of Contract/Breach of the Covenant of Good Faith and Fair Dealing (on behalf of all Plaintiffs and the Breach of Contract Class)

189. Plaintiffs repeat paragraphs 1 through 188 above.

190. Plaintiffs and Defendants have contracted for services as described in Comerica's Terms of Use and related documentation.

191. Defendants violated the contract by failing to adhere to the policies and procedures contained in the contract with respect to fraudulent and unauthorized transactions. Thus, Defendants have materially breached the express terms of their own form contract.

192. Plaintiffs and the members of the Breach of Contract Class have performed all, or substantially all, of the obligations imposed on them under the contracts, or those obligations have been waived by Defendants.

193. Plaintiffs and the members of the Breach of Contract Class sustained damages as a result of Defendants' breaches of contract.

194. Under the laws of the states at issue, good faith is an element of every contract. Whether by common law or statute, contracts include the obligation that all parties act in good faith and deal fairly with the other parties. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit – not merely the letter – of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

Evading the spirit of the bargain and abusing the power to specify terms are examples of a lack of good faith in the performance of a contract.

195. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes his conduct to be justified. A lack of good faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Defendants have breached the covenant of good faith and fair dealing through their policies and practices as alleged herein.

196. Plaintiffs and the Class members have performed all, or substantially all, of the obligations imposed on them under the Terms of Use.

197. Plaintiffs and members of the Breach of Contract Class have sustained damages as a result of Defendants' breach of the covenant of good faith and fair dealing.

198. Whether based on direct breaches of the contract, or violations of the contract as a result of the covenant of good faith and fair dealing, or both, Defendants should be required to make Plaintiffs and the Breach of Contract Class whole.

SECOND CLAIM FOR RELIEF

Violation of the Electronic Funds Transfer Act and Regulations including 15 U.S.C. § 1693f and 12 C.F.R. § 1005.6 (on behalf of all Plaintiffs and the Regulation E Class)

199. Plaintiffs repeat paragraphs 1 through 188 above.

200. Plaintiffs allege this claim on behalf of themselves and the Regulation E Class members who have been assessed at least one fraudulent transaction on their Direct Express® Debit MasterCard Card.

201. Plaintiffs, on behalf of themselves and the Regulation E Class, assert that Defendants failed to:

a. investigate alleged errors, determine whether errors have occurred, and report or mail the results of such investigation and determination to the consumer within ten business days as required by 15 U.S.C. § 1693f(a)(3);

b. promptly, but in no event more than one business day after it was determined that an error did occur in situations where one if found, correct the error as required by 15 U.S.C. § 1693f(b);

c. provide provisional credits to a customer's account in accordance with 15 U.S.C. § 1693f(c); or

d. deliver or mail to the consumer an explanation of their findings within three business days after the conclusion of the investigation in situations where Defendants determined that an error did not occur, and upon request of the consumer, promptly deliver or mail to the consumer reproductions of all documents which the financial institution relied on to conclude that such error did not occur as required by 15 U.S.C. § 1693f(d).

202. Plaintiffs, on behalf of themselves and the Regulation E Class, also assert that Defendants failed to limit a consumer's liability for an unauthorized electronic fund transfer or a series of related unauthorized transfers in violation of 12 C.F.R. § 1005.6(b).

203. Indeed, the aforementioned Interim Audit Report issued by the Department of the Treasury found that Defendants "received poor ratings in . . . regulatory compliance related to chargeback and dispute processing." Thus, Plaintiffs' allegations regarding violations of Regulation E are well founded.

204. As a result of Defendants' violations of Regulation E, Defendants are liable to Plaintiffs and the Regulation E Class for actual and statutory damages, pursuant to 15 U.S.C. § 1693f(e).

205. As a result of Defendants' violations of Regulation E, Defendants are liable to Plaintiffs and the Regulation E Class for actual and statutory damages and Plaintiffs and the Classes are entitled to recover costs of suit and their reasonable legal fees.

THIRD CLAIM FOR RELIEF

Negligence

(on behalf of all Plaintiffs and the Data Breach Class)

206. Plaintiffs repeat paragraphs 1 through 188 above.

207. Defendants owed a duty to Plaintiffs and all customers members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal information from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that customers' personal information in their possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

208. Defendants' duty to use reasonable care arose from several sources including, but not limited to, those described below.

209. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class

members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and other Class members would be harmed.

210. Defendants' duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendants. Various FTC publications and data security breach orders further form the basis of Defendants' duties.

211. Defendants also had a duty to safeguard the personal information of Plaintiffs and Class members and to promptly notify them of a breach because of state laws and statutes that require Defendants to reasonably safeguard sensitive personal information, as detailed herein.

212. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendants' misconduct.

213. Defendants breached the duties they owed to Plaintiffs and Class members described above and thus were negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal information of Plaintiffs and Class members; (b) detect the breach or breaches while ongoing; (c) maintain security systems consistent with industry

standards; and (d) disclose that Plaintiffs' and the Class members' personal information in Defendants' possession had been, or was reasonably believed to have been, stolen or compromised.

214. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, their personal information would not have been compromised.

215. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiffs' and Class members' injuries include:

a. theft of their personal information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach – including finding fraudulent charges, cancelling

and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. actual injuries flowing from the fraudulent transactions and identity theft suffered by Plaintiffs resulting from their personal information being placed in the hands of criminals;

i. damages to and diminution in value of their personal information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

j. continued risk of exposure to hackers and thieves of their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs and Class members.

FOURTH CLAIM FOR RELIEF

Negligence *Per Se*

(on behalf of all Plaintiffs and the Data Breach Class)

216. Plaintiffs repeat paragraphs 1 through 188 above.

217. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants of failing to use reasonable measures to protect personal information. Various FTC publications and orders also form the basis of Defendants' duties.

218. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personal information they obtained and stored and the foreseeable consequences of a data breach.

219. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

220. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

FIFTH CLAIM FOR RELIEF

State Consumer Protection Laws

A. Alabama

221. Plaintiffs repeat paragraphs 1 through 188 above.

222. Mr. Carnley is a citizen of Alabama and was also a citizen of Alabama when the fraudulent transactions occurred on his account. He brings this Count on his own behalf and on behalf of members of the Alabama Subclass.

223. The Alabama Unfair Trade Practices Act (AUTPA) prohibits the following conduct in trade or commerce:

> (2) Causing confusion or misunderstanding as to the source, sponsorship, approval, or certification of goods or services . . . .
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have . . . .
> (7) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another . . . .
> (9) Advertising goods or services with intent not to sell them as advertised . . . .
> (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

Ala. Code § 8-19-5.

224. Defendants' acts and omissions affect trade and commerce and affect sponsorship of goods and services in Alabama.

225. Defendants have committed acts of unfair competition in violation of Alabama Code Section 8-19-5. Defendants falsely represented to Mr. Carnley and the Alabama Subclass that personal and financial information provided to Direct Express® in sales transactions would be safe and secure from theft and unauthorized use when, in truth and fact, Direct Express® did not take reasonable and industry-standard measures to protect such personal and financial information from theft and misuse.

226. Defendants have violated Section 8-19-5(2) and (5) through their representations that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that it do not have . . . ."

227. Defendants have also violated Section 8-19-5(7) because they represented that their goods and services were of a particular standard, quality, or grade, when in truth and fact, they were not.

228. Defendants have also violated Section 8-19-5(9) because they induced transactions with consumers under the false auspices that they reasonably protected consumers' private data.

229. Defendants conducted the practices alleged herein in the course of their business, pursuant to standardized practices that they engaged in both before and after the Plaintiffs in this case were harmed, these acts have been repeated countless times, and many consumers were affected.

230. Defendants' misrepresentations and omissions were material to Mr. Carnley and the Alabama Subclass and were made knowingly and with reason to know that Mr. Carnley and the Alabama Subclass would rely on the misrepresentations and omissions.

231. Mr. Carnley and the Alabama Subclass reasonably relied on Defendants' misrepresentations and omissions and suffered harm as a result. Mr. Carnley and the Alabama Subclass were injured in fact by: fraudulent charges on their accounts; time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) inability to withdraw funds held in their accounts; (e) late fees and declined payment fees imposed as a result of failed payments; (f) the general nuisance and annoyance of dealing with all these issues resulting from the fraudulent transactions; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the fraudulent transactions, all of which have an ascertainable monetary value to be proven at trial.

232. Mr. Carnley and the Alabama Subclass seek actual and statutory damages, to the full extent permitted under applicable law.

B. <u>California</u>

233. Plaintiffs repeat paragraphs 1 through 188 above.

234. Mr. Simms is a citizen of California and was also a citizen of California when the fraudulent transactions occurred on his account. He brings this Count on his own behalf and on behalf of members of the California Subclass.

235. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

236. Defendants are businesses that own, maintain, and license Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

237. Businesses that own or license computerized data that includes Personal Information, including Social Security numbers, are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

238. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

239. Plaintiff and California Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered by Cal. Civ. Code § 1798.82.

240. Because Defendants reasonably believed that Plaintiff's and California Subclass members' Personal Information was acquired by unauthorized persons during the data breach, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

241. By failing to disclose the data breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82

242. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

243. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

244. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA"), is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property, or services to consumers primarily for personal, family, or household use.

245. Defendants are a "person" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

246. Plaintiff and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

247. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

248. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' Personal Information.

249. Had Defendants disclosed to Plaintiffs and Class members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

250. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

251. Plaintiff and the California Subclass have provided notice of their claims for damages to Defendants, in compliance with California Civil Code § 1782(a).

252. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

C. Colorado

253. Plaintiffs repeat paragraphs 1 through 188 above.

254. Mr. Tillman is a citizen of Colorado and was also a citizen of Colorado when the fraudulent transactions occurred on his account. He brings this Count on his own behalf and on behalf of members of the Colorado Subclass.

255. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

256. Plaintiff and Colorado Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

257. Defendants are required to accurately notify Plaintiff and Colorado Subclass members if they become aware of a breach of their data security systems in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

258. Because Defendants were aware of a breach of their security systems, they had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

259. By failing to disclose the data breach in a timely and accurate manner, Defendants violated Colo. Rev. Stat. § 6-1-716(2).

260. As a direct and proximate result of Defendants' violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

261. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief

D. Massachusetts

262. Plaintiffs repeat paragraphs 1 through 188 above.

263. Ms. Densmore is a citizen of Massachusetts and was also a citizen of Massachusetts when the fraudulent transactions occurred on her account. She brings this Count on his own behalf and on behalf of members of the Massachusetts Subclass.

264. Ms. Densmore's interactions with Defendants prior to the filing of this action satisfy the pre-suit demand for relief requirement on behalf of the Massachusetts Subclass.

265. Defendants operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

266. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of services in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), in at least the following ways:

a. Defendants misrepresented material facts to Ms. Densmore and the Massachusetts Subclass by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Massachusetts Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Defendants misrepresented material facts to Ms. Densmore and the Massachusetts Subclass by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Ms. Densmore's and the Massachusetts Subclass members' personal and financial information;

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Ms. Densmore and the Massachusetts Subclass members' personal and financial information;

d. Defendants engaged in unfair acts and practices by failing to maintain the privacy and security of Ms. Densmore's and the Massachusetts Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, the Massachusetts Right of Privacy Statute (Mass. Gen. Laws Ann. ch. 214, § 1B), and the Massachusetts data breach statute (Mass. Gen. Laws Ann. ch. 93H, § 3(a));

e. Defendants engaged in unfair acts and practices by failing to disclose the data breach to Massachusetts Subclass members in a timely and accurate manner, in violation of Mass. Gen. Laws Ann. ch. 93H, § 3(a);

f. Defendants engaged in unfair acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Massachusetts Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

267. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within the penumbra of common law, statutory, or other established concepts of unfairness.

268. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Massachusetts Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the Massachusetts Subclass.

269. As a direct and proximate result of Defendants' unlawful practices, Ms. Densmore and Massachusetts Subclass members suffered injury and/or damages.

270. Massachusetts Subclass members seek relief under Mass. Gen. Laws Ann. ch. 93A, § 9, including, but not limited to, actual damages, statutory damages, double or treble damages, injunctive and/or other equitable relief, and/or attorneys' fees and costs.

E. Nevada

271. Plaintiffs repeat paragraphs 1 through 188 above.

272. Mr. Katynski is a citizen of Nevada and was also a citizen of Nevada when the fraudulent transactions occurred on his account. He brings this Count on his own behalf and on behalf of members of the Nevada Subclass.

273. In the course of their business, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts, in at least the following ways:

a. Defendants misrepresented material facts to Mr. Katynski and the Nevada Subclass by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nevada Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

b. Defendants misrepresented material facts to Mr. Katynski and the Nevada Subclass by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Mr. Katynski and Nevada Subclass members' personal and financial information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Mr. Katynski and Nevada Subclass members' personal and financial information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

d. Defendants engaged in deceptive trade practices by failing to maintain the privacy and security of Mr. Katynski and Nevada Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, the Nevada Confidentiality and Disclosure of Information Statute (Nev. Rev. Stat. § 695F.410), and the Nevada data breach statute (Nev. Rev. Stat. Ann. § 603A.210);

e. Defendants engaged in deceptive trade practices by failing to disclose the data breach to Nevada Subclass members in a timely and accurate manner, in violation of Nev. Rev. Stat. Ann. § 603A.220(1);

f. Defendants engaged in deceptive trade practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Mr.

Katynski and Nevada Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

274. The above unlawful and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

275. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Mr. Katynski and Nevada Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Subclass.

276. As a direct and proximate result of Defendant's deceptive practices, Mr. Katynski and Nevada Subclass members suffered injury and/or damages.

277. Mr. Katynski and Nevada Subclass members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

F. North Carolina

278. Plaintiffs repeat paragraphs 1 through 188 above.

279. Ms. Paglia is a citizen of North Carolina and was a citizen when the data breach occurred. Ms. Paglia brings this Count on her own behalf and on behalf of members of the North Carolina Subclass.

280. Defendants constitute businesses that own or license computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

281. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

282. Defendants are required to accurately notify Plaintiff and North Carolina Subclass members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

283. Plaintiff's and North Carolina Subclass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

284. Because Defendants discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

285. By failing to disclose the data breach in a timely and accurate manner, Defendants violated N.C. Gen. Stat. § 75-65.

286. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

287. As a direct and proximate result of Defendants' violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

288. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

289. Defendants also advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

290. Defendants engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Personal Information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Fair Credit Reporting Act, 15 U.S.C. § 1681e, and The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the data breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

291. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

292. Defendants intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on these misrepresentations and omissions.

293. Had Defendants disclosed to Plaintiffs and Class members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

294. Defendants acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights.

295. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

296. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

H. South Carolina

297. Plaintiffs repeat paragraphs 1 through 188 above.

298. Mr. McPhail is a citizen of South Carolina and was a citizen when the data breach occurred. Mr. McPhail brings this Count on his own behalf and on behalf of members of the South Carolina Subclass.

299. Defendants are a "person" under S.C. Code Ann. § 39-5-10.

300. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ." S.C. Code Ann. § 39-5-20(a). Defendants' actions as set herein occurred in the conduct of trade or commerce.

301. In the course of their business, Defendants willfully failed to disclose and actively concealed their inadequate computer and data security, that they had suffered data breaches, and otherwise engaged in activities with a tendency or capacity to deceive. Defendants also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that

others rely upon such concealment, suppression, or omission, in connection with their provision of financial services.

302. Defendants knew they had taken inadequate measures to ensure the security and integrity of their computer and data systems and they knew they had suffered data breaches. Defendants knew this for an extended period of time, but concealed all of that information.

303. Defendants were also aware that they valued profits over the security of consumers' personal and financial information, and that they had suffered data breaches. Defendants concealed this information as well.

304. By failing to disclose that their computer and data security measures were inadequate, that they had suffered data breaches, and by presenting themselves as reputable financial companies that valued consumers' personal and financial information and stood behind consumers, Defendants engaged in deceptive business practices in violation of the South Carolina UTPA.

305. Defendants' unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Mr. McPhail and the South Carolina Subclass members, about the inadequacy of Defendants' computer and data security and the quality of the Comerica brand.

306. Defendants intentionally and knowingly misrepresented material facts regarding the security and integrity of their computer and data systems with an intent to mislead Plaintiff and the South Carolina Subclass.

307. Defendants knew or should have known that their conduct violated the South Carolina UTPA.

308. As alleged above, Defendants made material statements about the security and integrity of their computer and data systems and the Comerica/Direct Express® brand that were either false or misleading.

309. Defendants owed Mr. McPhail and the South Carolina Subclass a duty to disclose the true nature of their computer and data systems, and the devaluing of data security because Defendants:

a. Possessed exclusive knowledge that they valued profits over the security of consumers' data;

b. Intentionally concealed the foregoing from Mr. McPhail and the South Carolina Subclass; and/or

c. Made incomplete representations about the security and integrity of their computer and data systems generally, and their data breaches, while purposefully withholding material facts from Mr. McPhail and the South Carolina Subclass that contradicted these representations.

310. Defendants' fraudulent claims of security and the true nature of their computer and data system security were material to Mr. McPhail and the South Carolina Subclass.

311. Mr. McPhail and the South Carolina Subclass suffered ascertainable loss caused by Defendants' misrepresentations and their concealment of and failure to disclose material information. Mr. McPhail and South Carolina Subclass members' personal and financial information would not have been stolen but for Defendants' violations of the South Carolina UTPA.

312. Defendants had an ongoing duty to all customers to refrain from unfair and deceptive practices under the South Carolina UTPA. Mr. McPhail and the South Carolina Subclass

members suffered ascertainable loss in the form of the theft of their personal and financial information as a result of Defendants' deceptive and unfair acts and practices made in the course of their business.

313. Defendants' violations present a continuing risk to Mr. McPhail and the South Carolina Subclass as well as to the general public. Defendants' unlawful acts and practices complained of herein affect the public interest.

314. As a direct and proximate result of Defendants' violations of the South Carolina UTPA, Mr. McPhail and the South Carolina Subclass have suffered injury-in-fact and/or actual damage.

315. Pursuant to S.C. Code Ann. § 39-5-140(a), Mr. McPhail and the South Carolina Subclass seek monetary relief against Defendants to recover for their economic losses. Because Defendants' actions were willful and knowing, Mr. McPhail and the South Carolina Subclass members' damages should be trebled.

316. Plaintiff and the South Carolina Subclass further allege that Defendants' malicious and deliberate conduct warrants an assessment of punitive damages because Defendants carried out despicable conduct with willful and conscious disregard of the rights and safety of others, subjecting Mr. McPhail and the South Carolina Subclass to cruel and unjust hardship as a result. Defendants intentionally and willfully misrepresented the security and integrity of their computer and data systems, deceived Mr. McPhail and the South Carolina Subclass, and concealed material facts that only Defendants knew. Defendants' unlawful conduct constitutes malice, oppression, and fraud warranting punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Classes demand a jury trial on all claims so triable and judgment which includes the following:

1. Certification of the Classes under Rule 23 and appointment of Plaintiffs as class representatives and Plaintiffs' counsel as class counsel;

2. Restitution of all monies lost by Plaintiffs and the Classes as a result of the wrongs alleged herein in an amount to be determined at trial;

3. Disgorgement of the ill-gotten gains derived by Defendants from their misconduct;

4. Actual damages in an amount proven at trial;

5. Punitive and exemplary damages;

6. Pre-judgment interest at the maximum rate permitted by applicable law;

7. Reimbursement of all fees, expenses, and costs of Plaintiffs in connection with this action, including reasonable attorneys' fees pursuant to applicable law; and

8. Such other relief as this Court deems just and proper.

DATED this 5th day of September, 2019.

Respectfully Submitted

By: s/ Allen R. Vaught

Allen R. Vaught
TX Bar No. 24004966
Vaught Firm, LLC
6122 Palo Pinto Ave.
Dallas, TX 75214
E-Mail: allen@vaughtfirm.com
Phone: (214) 675-8603
Fax: (214) 261-5159

WEBB, KLASE & LEMOND, LLC

E. Adam Webb*
Georgia Bar No. 743910
G. Franklin Lemond, Jr.*
Georgia Bar No. 141315
1900 The Exchange, S.E.
Suite 480
Atlanta, Georgia 30339
(770) 444-9325
(770) 217-9950 (fax)
Adam@WebbLLC.com
Franklin@WebbLLC.com

Attorneys for Plaintiffs
(* Motion for *Pro Hac Vice* Admission to be filed.)